

## Design and Implementation of a Door Card Access System Using Internet of Things Technology

Oluwasola S. Maitanmi<sup>1\*</sup>, Akinniran O. Oke<sup>2</sup>, Ayorinde Peters Oduroye<sup>3</sup>, Adesoji Adedeji Adegbola<sup>4</sup>,  
Olubukola D. Adekola<sup>5</sup>, Ajao Joseph Oluwatosin<sup>6</sup>, Kikelomo Ibiwumi Okesola<sup>7</sup>, Michael Agbaje<sup>8</sup>,  
Funmilayo A. Sanusi<sup>9</sup>, Akintoye A. Onamade<sup>10</sup>, Olusegun Gbenga Lala<sup>11</sup>

Submitted: 13/05/2024 Revised: 24/06/2024 Accepted: 02/07/2024

**Abstract:** The advent of technology has helped to ease a number of manual activities that takes place globally, including our homes. Smart homes are automation systems integrated with Internet of Things (IoT) that controls several home appliances efficiently. IoT systems employ various sensors, programming, and microcontroller combination for controlling the home electronic systems. These systems are becoming an essential part of today's life as they allow users to monitor, control, and manage home appliances automatically. Smart homes can implement burglary detection systems, fire alarms, water handout control, automatic safety alerts for gas leakage, smart meter-based electricity control, and remote temperature control for heating/cooling. This paper focused on the automation of a door access system using smart card. The system integrates Arduino Uno, ESP32 board, a solenoid lock, and smart card to provide secure and efficient access control. It involved the design and construction of the hardware components, including wiring and assembly, as well as the development of software for card authentication and door control.

**Keywords:** Arduino, Circuit diagram, Frequency Identification (RFID), Internet of Things (IOT), Smart card.

### 1. Introduction

The world today is the world of technology. Each and every one is addicted to it, consciously or unconsciously.

<sup>1</sup>Associate Professor of Computer Science (Software Engineering), Software Engineering, Babcock University, Ilishan Remo, Ogun State, Nigeria.  
ORCID ID: 0000-0002-0217-0543

<sup>2</sup>Software Security Director, Turnkey Kinetics Services, Winnipeg, Manitoba ORCID ID: 0009-0003-7450-5132

<sup>3</sup>Senior Lecturer, Computer Science Department, Caleb University, Imota, Lagos State, Nigeria.  
ORCID ID: 0000-0001-8755-9816

<sup>4</sup>Assistant Lecturer, Software Engineering Department, Babcock University, Ilishan Remo, Ogun State, Nigeria.  
ORCID ID: 0000-0003-1312-8938

<sup>5</sup>Associate Professor of Software Engineering, Babcock University, Ilishan Remo, Ogun State, Nigeria.  
ORCID ID: 0000-0002-5495-6791

<sup>6</sup>ICT Coordinator, Babcock University Postgraduate School, Ilishan Remo, Ogun State, Nigeria.  
ORCID ID: 0009-0009-0216-7625

<sup>7</sup>Lecture I, Software Engineering Department, Babcock University, Ilishan Remo, Ogun State, Nigeria.  
ORCID ID: 0000-0003-0944-1497

<sup>8</sup>Associate Professor of Computer Science, Babcock University, Ilishan Remo, Ogun State, Nigeria.  
ORCID ID: 0000-0003-3789-9542

<sup>9</sup>Senior Lecturer, Computer Science Department, Mountain Top University, Department of Computer Science & Mathematics, Ogun State, Nigeria  
ORCID ID: 0000-0001-5794-3657

<sup>10</sup>Associate Professor, Computer Science Department Adeleke University, Ede, Osun State, Nigeria.  
ORCID ID: 0000-0002-5307-4754

<sup>11</sup>Associate Professor, Faculty of Science, Department of Information Technology, Adeleke University, Ede, Osun State, Nigeria.  
ORCID ID: 0000-0002-5766-0072

\* Corresponding Author Email: maitanmio@babcock.edu.ng

A few years back, the Internet was only available to a few nations; today, it is reaching every corner of the globe. With the advancement of the Internet, each and everything is being connected to it; each and every person can access data from any point on the globe.

In the same way, devices like Electronic Appliances, Electrical Equipment, Air Conditioners, Home Lighting Systems, etc. can also be connected to each other through the Internet and can be controlled from any corner of the globe. This network of things can be termed as IoT, i.e. the Internet of Things [1].

At present, a door to any building i.e. Home, Office, Factory, School, etc. is opened by using a 'Key'. There is always a chance of fake key imitation and manual theft of the keys. Hence a person can use it and easily

access the restricted area. To overcome this situation, there are a number of technologies available, one of these is a door card access system. In this paper, the use of a card for opening the locks of doors works as an extra layer of security, as it is harder to impersonate a card than a key. The functioning of the door card access system can be done in two ways, i.e. inside an area and from afar. The inside door card access is a single door which will be opened by a valid card which will activate the mechanism, and the door will be opened. The more secured door card access is an access from the afar, i.e. it is open via IoT Technology, where the door access will be controlled using a Webpage. A person opens the door by tapping on

a button, and the camera will capture a person's image and send it to the page of the owner of the door, who will have the authority to reject or accept the entry [2].

### 1.1 Statement of the Problem

Burglary is the second most reported crime type after Assault, with a total of reported cases of 693,631 over the years [3]. Losing a key is a common problem, and replacing traditional keys can be inconvenient and costly. To ensure consistent home security, occupants typically strive to lock the door whenever they leave or rest inside the house. Unfortunately, instances of forgetting to lock the door due to time constraints or uncertainty about its status are not uncommon, posing a significant threat to home security. [4] proposed and implemented a low-cost architecture using radio frequency (RF) based communication in a household to create an IoT-enabled smart home security system. While the concept was innovative, the weakness of this approach was its over-reliance on smartphone technology and the inability to alert users in the event of trespassing. In response to the increasing security risks associated with traditional physical keys and digital door systems, there is a growing need for a more robust and convenient access control solution for homes and offices. This paper focused on developing a solution that offers robust authentication, convenience, and effective protection against unauthorized access, ultimately reducing the risk of break-ins and improving overall security.

The specific objectives of the article are:

1. develop a secure user authentication method that makes use of card for verification which has the following functions:
2. real-time monitoring of access events, including entry and exit timestamps, user identities, and any unauthorized attempts.
3. ability to add, modify, or delete authorized users, assign different access levels, and keep a record of user activities.
4. implementation of the above was ensured.

### 2. Literature review

The world envisions a future where every gadget is interconnected to the Internet, forming an intelligent network where anything can be controlled from anywhere [2]. Machines connect, gather, and send data through the Internet of Things (IoT). Due to these growing demands, researchers, technologists, and engineer are actively identifying solutions to various problems or concerns using IoT technology. One such need is security management, specifically access control. In this age of digitization, where everything might be tracked and analyzed skillfully, ensuring the safety of information and resources becomes a top priority [5].

Access control systems are primarily focused on prohibiting unauthorized access to sensitive zones, resources, and information. These systems have evolved and accelerated from traditional lock-and-key systems to advanced systems known as smart card access control systems. There are various opportunities to integrate IoT technology in access control systems using advanced technologies and innovative gadgets. One such opportunity is to utilize Arduino technology to design and deploy an access control system. Arduino is an open-source platform comprised of computer hardware, software, and microcontrollers widely used in IoT applications.

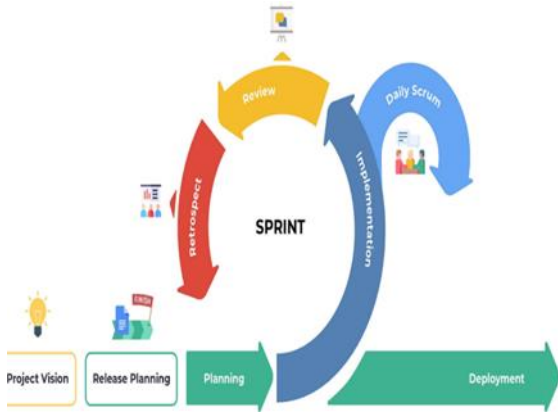
### 2.1 Overview of IoT Technology

Internet of Things (IoT) technology provides a method of remote surveillance of physical infrastructures and monitoring, management, In the last few years, the IoT has become one of the most discussed terms in technological development. It has the potential to change our daily lives and our understanding of the world in which we live. The IoT network consists of physical things equipped with sensors to facilitate connectivity. These physical things are linked to the internet, where data generated, received, or captured by them is stored and made available for processing. This technology paves the way for a wide range of applications of connected physical things to change the way we look at and handle things [1].

The IoT network contains early identification, decision making, and intervention to avoid natural calamities or human-made hazards. Most mechanical systems are hand-operated, helmet-controlled, and body-controlled by a network that is either wired or wireless. This technology is emerging in many fields, including agriculture, healthcare, home automation, and industrial automation. Most hospitals are introducing the smart medical system to store a patient's medical history and track them every time they have a check-up. In a traditional panel, the entry or exit of more than six nonauthorized people is monitored by a person by continuously observing the CCTV footage. A bi-directional alarm signaling system is used, which creates a disturbance or alerts nearby persons whenever unauthorized entry is found. This makes unauthorized entry easy, because continuous surveillance is not guaranteed [5].

### 3. System Design

The design refers to how a system works and the series of components that constitute the design. The design of this article used the scrum process model as demonstrated in Fig. 1.



**Fig. 1** Scrum process Model Diagram. Source:[6]

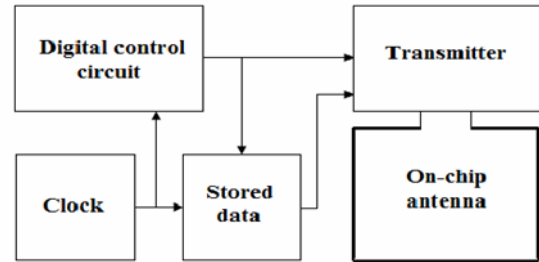
Creating a process model diagram for the design and implementation of a Door Pin Access system using IoT involves outlining the sequential steps which involved seven (7) stages of the development lifecycle as elaborated below:

- the planning phase evaluates the potential risks associated with the system implementation and operation, plan the required resources, including hardware, software, and personnel; create a budget and timeline for the project;
- requirements gathering and analysis phase accommodates the identification of the stakeholders' needs and system requirements, definition of functional and non-functional requirements for the system;
- design phase includes the system architecture design; designing the overall system architecture, including IoT components, databases, and communication protocols; user interface design involved the creation of the interface through which users interact with the system (e.g., mobile application, web interface); security protocols design which determines encryption standards, authentication methods, and access control mechanisms;
- development phase integrate selected hardware components into the system and software development takes care of the developed firmware or software for IoT devices, authentication protocols, as well as cloud/server-side applications;
- testing phase performed rigorous testing of the entire system such as the functional testing, security testing and usability testing;
- deployment phase integrates all components and subsystems into a cohesive system, deployed the system in a controlled environment and
- maintenance phase sets up mechanisms for continuous monitoring of the system's performance, security, user feedback and provide ongoing maintenance and support for updates, bug fixes, and improvements.

### 3.1 System Architectural of the Design

### 3.2 Radio Frequency Identification (RFID) tag

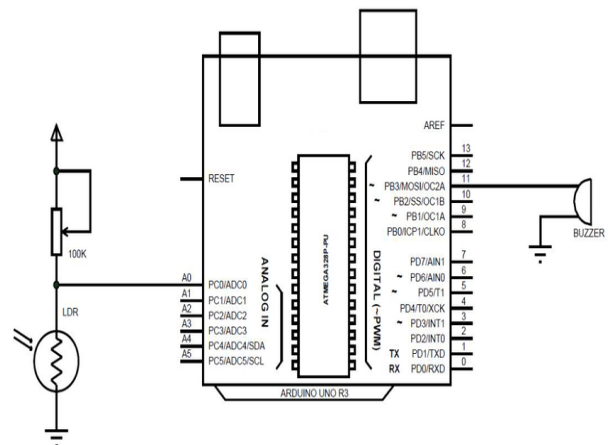
The RFID tags serve as unique identifiers for users. Each user is provided with an RFID tag encoded with specific access permissions, allowing them to interact with the system. The system's IoT infrastructure includes RFID readers at the door, which communicate with the central system to verify the tag's authenticity and grant or deny access based on the encoded permissions as demonstrated in Fig 2.



**Fig 2.** Block Diagram of FRID tag

### 3.3 Arduino Uno R3

The Arduino Uno R3 is utilized as the central controller in the design of the Door Pin Access system. It manages input from RFID tags and sensors while interfacing with IoT modules for connectivity. Through the Arduino Uno R3, the system verifies access, and controls the locking mechanism, integrating IoT technology to enable remote access and monitoring capabilities via cloud-based platforms or network connections as depicted in Fig. 3.



**Fig. 3.** Circuit diagram of Arduino Uno R3

### 3.4 ESP32

The ESP32 serves as a powerful microcontroller platform leveraging its Wi-Fi and Bluetooth capabilities, the ESP32 can interface with various sensors, and door locks, enabling seamless communication within the IoT ecosystem as seen in Fig. 4.

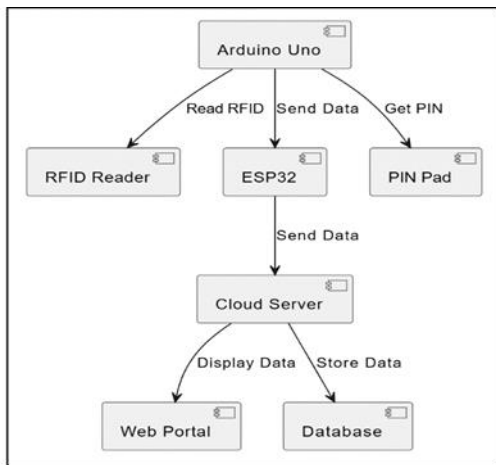


Fig 4. Schematic Diagram of ESP32

### 3.5 RFID-based-security-system

The RFID-based security system of the article integrates RFID readers with IoT controllers and door locks. RFID tags or cards are assigned to users, enabling seamless access through authentication when presented to the reader as seen in Fig 5. The IoT infrastructure manages user access permissions, logs entry attempts, and facilitates remote access control, ensuring a secure and streamlined entry system.

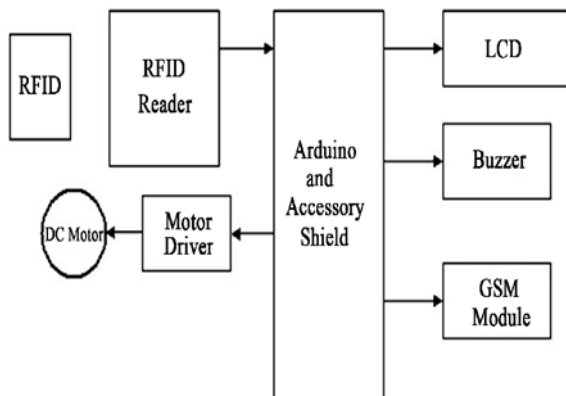


Fig 5. Block diagram of RFID based security system

## 4. Result & Discussion of findings

All the above-described components were integrated to the cloud server (manage user credentials and authenticate users based on the data received from the ESP32 microcontroller), web portal (provide the system administrators with a user-friendly interface for viewing user logs) and the database (store user credentials including RFID tag information) as described in Fig 6.

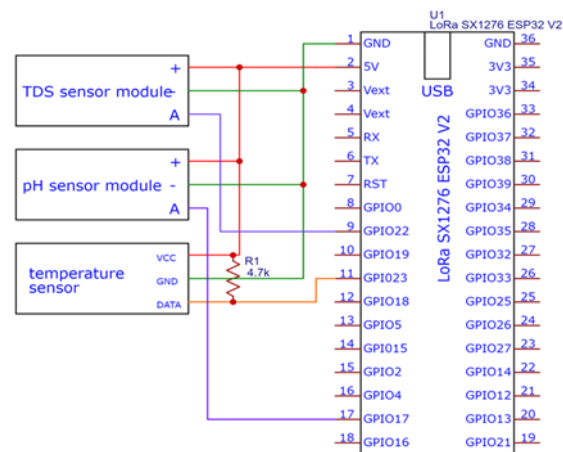


Fig 6. System Architecture Diagram

## 4.1 Use Case Diagrams

The system is designed for use by two categories of users: Public and Admins. Public users when given temporary access to the system; they must be allowed by the admin to use the system. Admin users have the most privileges and have access to admin dashboard with features like managing access control these was demonstrated use case diagram as seen in Fig 7.

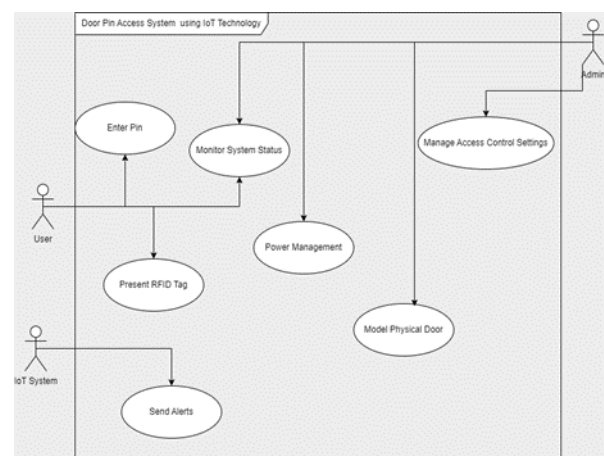


Fig 7. Use Case diagram of the architecture









## 4.2 Report and Discussion

The Smart Access Control article integrates various components to provide secure access control to a door model using RFID card authentication. The system employs an ESP32 microcontroller for IoT control, an RFID card reader, RFID cards for access control, a solenoid door lock, a buzzer, and an RGB LED indicator. Detailed operation and functionality are outlined in Table 1.

### Components:

Table 1. Showing various components and meaning

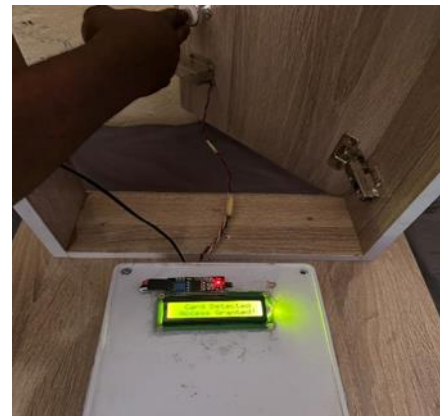
S/N	Components	Name & Functions
-----	------------	------------------

1		ESP32. Microcontroller: Manages system operations, including Wi-Fi connectivity and access control logic.
2		RFID Card Reader: Reads RFID cards for user authentication.
3		RFID Cards: Two cards grant access, while one card denies access, each uniquely assigned to individuals.
4		Solenoid Door Lock: Controls physical access to the door
5		Buzzer: Provides audible feedback for access status.
6		RGB LED Indicator: Provides visual feedback for access status.
7		Motor Driver shield: Controls the solenoid door lock.
8		12V Power adapter: Power supply for the entire system.

### 4.3 Operational procedures of the door using scan RFID card

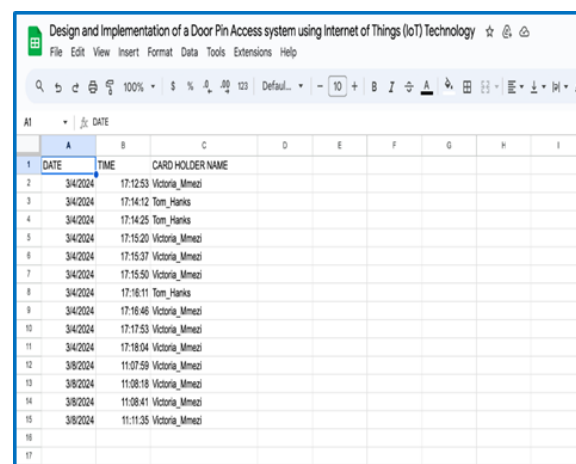
When an RFID card is scanned, the buzzer emits a double beep. The system checks the scanned card against its program to determine access status, if access is granted, the solenoid door lock opens for four (4) seconds, and the green LED lights up as seen in Fig. 8. However, if access

is denied, the solenoid door lock remains shut, the buzzer emits a continuous beep for five (5) seconds, and the red LED lights up for five (5) seconds simultaneously.



**Fig. 8** Showing the demonstration using the scan RFID card

Access events, including the cardholder's name, timestamp, and authorization status (access granted or denied), are logged in real-time to an Excel sheet hosted in the cloud as shown in Fig 9.



DATE	TIME	CARD HOLDER NAME
3/4/2024	17:12:53	Victoria_Mmezi
3/4/2024	17:14:12	Tom_Hanks
3/4/2024	17:14:25	Tom_Hanks
3/4/2024	17:15:20	Victoria_Mmezi
3/4/2024	17:15:37	Victoria_Mmezi
3/4/2024	17:15:50	Victoria_Mmezi
3/4/2024	17:16:11	Tom_Hanks
3/4/2024	17:16:46	Victoria_Mmezi
3/4/2024	17:17:53	Victoria_Mmezi
3/4/2024	17:18:04	Victoria_Mmezi
3/8/2024	11:07:59	Victoria_Mmezi
3/8/2024	11:08:18	Victoria_Mmezi
3/8/2024	11:08:41	Victoria_Mmezi
3/8/2024	11:11:35	Victoria_Mmezi

**Fig. 9.** Excel sheet showing logged access events

### 5. Conclusion

Door access systems using Internet of Things (IoT) Technology represents a significant step toward the improvement of traditional door access control systems. Unlike the traditional method which is reliant on physical keys, this system provides a more modern approach to access control which can stop a number of challenges as iterated in the paper. This system uses RFID tags as digital keys which replaces the need for traditional physical keys which simplifies the access process but also enhances security measures. With RFID tags, users can gain entry by simply placing their tag to the designated scanner.

### References

[1] S. Walia, T. Iyer, S. Tripathi, and A. Vanaparthi "Safe and Secure Smart Home using Cisco Packet

- Tracer”. 2023  
<https://doi.org/10.48550/arXiv.2304.11827>
- [2] Mhlaba, and M. Masinde “Implementation of Middleware for Internet of Things in Asset Tracking Applications: In-lining Approach” IEEE 13th International Conference on Industrial Informatics (INDIN), 2015, pp. 460-469, doi:10.1109/INDIN.2015.7281778
- [3] P. Oguntunde, O.O. Ojo, H. I. Okagbue, and O. A. Oguntunde, O. A. “Analysis of selected crime data in Nigeria” *ScienceDirect*, 19, 2018, pp. 1242-1249. <https://doi.org/10.1016/j.dib.2018.05.143>.
- [4] S. Falohun, B.O. Makinde, O.A. Adegbola, T.H. Akin-Olayemi, A.E. Adeyege, A. E., Adeosun, and B.D. Akande, “Design and construction of a Smart Door lock with an Embedded Spy-Camera”. *Journal of Multidisciplinary Engineering Science and Technology (JMEST)*, 2021, Vol. 8, No 7.
- [5] S. Pal, A. Dorri, and R. Jurdak “Blockchain for IoT Access Control: Recent Trends and Future Research Directions” *Journal of Network and Computer Applications*, 2021, p. 203, 103371. <https://doi.org/10.1016/j.jnca.2022.103371>.
- [6] M.A. Hoque “*Design and Implementation of an IoT-Based Smart Home Security System*. Atlantis Press” 2019  
<https://www.atlantispress.com/journals/ijndc/125905847/view>